REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following remarks is respectfully requested.

Claims 1-3 and 6-26 are currently active. No claims are amended, added or canceled by the present amendment.

In the outstanding Official Action, Claims 1-9 and 11-18 were rejected under 35 U.S.C. § 102(e) as anticipated by European Patent Application EP 0982895 to Shimizu et al. (herein "Shimizu"); and Claim 10 was rejected under 35 U.S.C. § 103(a) as unpatentable over Shimizu in view of U.S. Patent No. 5,933,501 to Leppek. Applicants respectfully traverse those rejections.

Before discussing the applied prior art, it is believed that a brief review of the background of the invention and the present invention would be helpful. Applicants' invention eliminates the need to use expanded keys in decryption in an order reversed from that for encryption, i.e., in order from expanded key (n) to expanded key (1). In conventional decryption apparatuses, having an expanded key scheduling section configured similar to that shown in Applicants' FIG. 48, expanded keys are generated in order from expanded key (1) to expanded key (n). Because of this, prior to processing of the data randomizing section, there has been a need to generate all the expanded keys and store them in a memory. However, with a conventional approach there has been a problem that a device with limited hardware resources, for example an IC card, does not have sufficient storage space for storing all the expanded keys required for decryption.[1]

In contrast to the conventional systems, Applicants' Claim 1 is directed to an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for

1 Specification at page 4, lines 10-25.

encryption and in a reversed order in a data randomizing process for decryption. The encryption apparatus includes, in part, a plurality of round processing circuits that comprise at least a pair of round processing circuits having inverse round functions. Independent Claims 11, 13 and 15-18 include similar features.

In a non-limiting example, Applicants' Figure 1 shows an embodiment of an encryption apparatus as recited in Claim 1, including a plurality of round processing circuits (31) that comprise at least a pair of round processing circuits (31) having inverse round functions such that the sub key output from the round processing circuit of the last stage may be the common key which is input to the round processing circuit of the first stage. Since the inverse functions are used, it is easy to make the sub key output from the round processing circuit of the last stage be the common key.

In order to output the same common key which is input to the first stage of the expanded key scheduling section (3) from the last state of the expanded key scheduling section 3, the plurality of round processing circuits (31) may comprise at least a pair of round processing circuits (31) having inverse round functions.

In particular, to generate expanded keys for decryption in order from expanded key (1) to expanded key (n), a series of round functions may be set so that a value corresponding to an output at the last stage for encryption coincides with an original common key. That is, the expanded keys may be generated such that a series of round functions for decryption are a series of inverse functions of the round functions for encryption. Due to this claimed configuration, in both encryption and decryption it is possible to generate an expanded key from a common key in an on-the-fly manner without incurring the unnecessary delay time or storage capacity that may be required by conventional systems.[2]

[2] Specification at page 25, lines 12-25.

Applicants' respectfully submit that Shimizu does not teach or suggest a plurality of round processing circuits that comprise at least a pair of round processing circuits having inverse round functions. In particular, Applicants' respectfully traverse the assertion in the outstanding Office Action that Shimizu teaches that at least a pair of round processing circuits has inverse round function by the fact that the round functions employ involution functions.[3] Shimizu merely teaches that "there is no limitation on a function to be employed in the key conversion section with the exception that an original key is converted by using an involution function and further it is not necessary for an encryption key and a decryption key to be same."[4] As is clear from the underlined phrases, Shimizu does not aim to make the encryption key equal to the decryption key. Therefore, Shimizu does not assert that the subkey output from the round processing circuit of a last stage is a common key.

Further, Shimizu indicates that "an involution function allows common use of circuitry between an encryption conversion and a decryption conversion."[5] Accordingly, an involution function refers to $fk_1 = fk_1^{-1}$, $fk_2 = fk_2^{-1}$, ... $fk_n = fk_n^{-1}$, whereas a pair of round processing circuits having inverse round functions means $f_1 = f_n^{-1}$. Thus, Shimizu does not mention a pair of round processing circuits having inverse round functions. Moreover, the present invention does not aim to allow common use of circuitry between an encryption conversion and a decryption conversion, as discussed by Shimizu.

In addition, Shimizu does not generate expanded keys for decryption in order from expanded key (1) to expanded key (n). In Shimizu, the extended keys are generated for encryption in order from the extended key K1 to the extended key Kn, as shown in Shimizu's FIG. 2, and the extended keys are generated for decryption in order from the extended key Kn to the extended key K1, as shown in Shimizu's FIG. 3. Stated another way, Shimizu involves

[3] Office Action at page 5, lines 6-10.
[4] Shimizu at column 3, lines 28-33 (emphasis added).
[5] Shimizu at column 8, lines 40-42.

the conventional problem shown in Applicants' FIG. 48. Therefore, at least a pair of round processing circuits having inverse round functions is not taught or suggested by Shimizu. Accordingly, it is respectfully submitted that Shimizu does not teach or suggest "the plurality of round processing circuits comprise at least a pair of round processing circuits having inverse round functions," as recited in independent Claim 1, and as similarly recited in independent Claims 11, 13 and 15-18.

Accordingly, Applicants respectfully submit that independent Claims 1, 11, 13 and 15-18, and claims depending therefrom, patentably define over Shimizu. Thus, it is respectfully requested the rejection of Claims 1-9 and 11-18 under 35 U.S.C. § 102(e) as anticipated by Shimizu be withdrawn.

In addition, Applicants respectfully traverse the rejection of Claim 10 under 35 U.S.C. § 103(a) as unpatentable over Shimizu in view of Leppek.

As discussed above, Claim 1 is believed to patentably define over Shimizu, and Claim 10 depends from Claim 1. Further, Applicants respectfully submit that Leppek does not teach or suggest the claimed features lacking in the disclosure of Shimizu. Accordingly, Applicants respectfully request the rejection of Claim 10 under 35 U.S.C. § 103(a) also be withdrawn.

Accordingly, it is believed that independent Claims 1, 11, 13 and 15-18, and claims depending therefrom, are allowable.

Consequently, in light of the above discussion no further issues are believed to be outstanding, and the present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Zachary S. Stern
Registration No. 54,719

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK:ZSS:dnf

I:\ATTY\ZS\21'S\211\211428US\211428 AMENDMENT 121905.DOC